UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,416	10/19/2006	Stephan J. Engberg	606-128-PCT-PA	9357

22145 7590 04/13/2010

KLEIN, O'Neill & SINGH, LLP
18200 Von Karman Avenue
Suite 725
IRVINE, CA 92612

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
04/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,416	ENGBERG, STEPHAN J.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-27 and 29-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-27 and 29-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application 10/575416 filed on 12/18/2009.

Claims 1-19 and 28 have been cancelled.

Claims 20-27, 29-30, 32-34, 36, and 38-39 have been amended.

Claims 20-27 and 29-39 have been examined and are pending.

Response to Arguments

Applicant's arguments, see pages 8-9, filed 12/18/2009, with respect to the objection of claim 32 have been fully considered and are persuasive. The objection of the specification has been withdrawn due amendment.

Applicant's arguments, see page 9, filed 12/18/2009, with respect to the specification have been fully considered and are persuasive. The objection of the specification has been withdrawn due amendment of the claim.

Applicant's arguments, see pages 9-10, filed 12/18/2009, with respect to the 35 U.S.C. § 112, 2nd rejection of claims 20-32 and 33-39 have been fully considered. The 35 U.S.C. § 112, 2nd rejection of claims 20-32 have been withdrawn due to amendment.

Applicant's arguments, see pages 9-10, filed 12/18/2009, with respect to the 35 U.S.C. § 112, 2nd rejection of claims 20-32 have been fully considered. The 35 U.S.C. § 112, 2nd rejection of claims 20-32 have been withdrawn due to amendment.

Applicant's arguments, see pages 9-10, filed 12/18/2009, with respect to the 35 U.S.C. § 112, 2nd rejection of claims 33-39 have been fully considered but they are not persuasive. The 35 U.S.C. § 112, 2nd rejection of claims 33-39 is maintained for the following reason:

The Applicant points out "in the paragraphs of [0113-0115] of the publication application, including storage of *"one-way encoded version of the biometric template.""* that supports *"means for verifying authentication"*. However, *"one-way encoded version of the biometric template*" is insufficient evidence to support the structure for *"means for verifying authentication"*.

Applicant's arguments, see pages 10-12, filed 12/18/2009 have been fully considered but they are not persuasive *(i.e. for the Second ground rejection under 35 U.S.C. 103).*
The Applicant argues the following:

(a) Engberg-1 does not teach amended 20 recites "providing an authentication of said chip card relative to the privacy reference point"; Engberg-1 does not provide disclosure to make a prima facie case of obviousness; Amended claim 20 recites "establishing a first communication path from said chip card privacy reference point." Engberg-1 does not appear to teach use of chip card. The Office action does not make a prima facie case of obviousness based on the combination of Engberg-1 and Pfitzmann.

The Examiner respectfully disagrees for the following reasons:

Per (a):

Engberg-1 teaches,

establishing a first communication path from said chip card to said privacy reference point *[Engberg-1: abstract: pg. 6, lines 3-12; providing a first virtual identifier of the first legal entity to the second legal entity, and establishing a communication path in according with a set of communication Rules specified by the first legal entity; See also; pg. 17; "The mobile processing and memory unit according to the fourth aspect of the invention may comprises SmartCard enabling Zero-knowledge authentication; pgs. 33, 56, 58, 76; Smartcard (i.e. chip card)];*

providing an authentication of the said chip card relative to the privacy reference point *[Engberg-1: abstract; pg. 6 line 21 to pg. 7, line 11; providing second legal entity with authentication or profile information related to said communication path and/or first legal entity; A preferred embodiment involves providing a Virtual Identifier equaling establishing an authenticated yet anonymous session in any kind of communication path; See also pg. 16, line 5 to pg. 17, line 8; authentication unit enabling the first client establishing a first virtual identity having a first virtual communication channel and establishing a rule based communication routing scheme for the privacy communication channel; pg. 56; tamper-safe SmartCards with a encryption authentication mechanism that can be either standard signature or a more complex zero-knowledge authentication procedure. See for instance [S.A. Brands 1999 PHD thesis later published as "Re-thinking Public and Digital Certificate", MIT Press, 2000, ISBN 0-262-02491-8"];*

In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where

there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Engberg-1 by including the teaching of Pfitzmann because it would provide a different transaction pseudonym is used, e.g. randomly generated transaction numbers for online-banking. Thus, there is at least no possibility to link different transactions by equality of pseudonyms. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible *[Pfitzmann, pg. 6, transaction pseudonym section]*.

Claim Rejections - 35 USC § 112

> The following is a quotation of the second paragraph of 35 U.S.C. 112:
>
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 33-39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 33, have been in valid as indefinite because the claims recite "*means for*" languages (*"**means for verifying** authentication"...)* and there is no structure disclosed in the specification. *"If there is no structure in the specification corresponding to the means-plus-*

function limitation in the claims, the claims will be found invalid as indefinite." Biomedino, LLC vs. Waters Technology Corp., 490 F.3d 946, 950 (Fed. Cir. 2007).

Claims 37, have been in valid as indefinite because the claims recite "*means for*" languages (*"**means for verifying employs data** selected from a group of "*) and there is no structure disclosed in the specification. *"If there is no structure in the specification corresponding to the means-plus-function limitation in the claims, the claims will be found invalid as indefinite." Biomedino, LLC vs. Waters Technology Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007).

Claims 34-39 are dependent on claim 33, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

The Examiner kindly requests the Applicant to point out and explain with specificity (i.e. column and line) in the specification where it describes/supports the aforementioned limitation (Emphasis added).

(A) First ground rejection:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 20-27, 29-31, and 33-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over by **Herz** et al. (5,754,938) in view of **Andreas Pfitzmann** et al, Anonymity, *Unobservability, and Pseudonymity - A Proposal for Terminology, LNCS 2009, pages 1-9, 2001,* further in view of **Engberg** et al. ("Privacy Authentication – persistent non-identification in Ubiquitous environments", August 18, 2002, pages 1-6).

As per claim 20:

Herz teaches a method of establishing a communication path in a data communication network from a first identity device *[[a chip card associated with a client]]*, comprising the steps of:

(a) providing a privacy reference point in said data communication network **[Herz: Col. 32, lines 3-65; "our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the implementation of a set of one or more proxy servers distributed throughout the network N. …. Proxy servers may be the same or different"; *a proxy server is functioned as private reference point*]**, *[[said privacy reference point configured for use in one transaction]].*

(b) establishing a first communication path from the first identity device *[[chip card]]* to said privacy reference point **[Herz: Col. 31, lines 48-55, "A pseudonym is an artifact that allows a service provider to communicate with users and build and accumulate records of their preferences over time, while at the same time remaining ignorant of the users' true**

identities, so that users can keep their purchases or preferences private"; *a user's true identity is equivalent to a first identity entity*];

(c) providing an authentication of said first identity device *[[chip card]]* relative to the privacy reference point **[Herz: Col. 30, line 39-43; Col. 37, lines 48-53; "The proxy server may verify those credentials and make appropriate modifications to the user's profile as required by these credentials such as recording the user's new demographic status as an adult. It may also store those credentials, so that it can present them to service providers on the user's behalf"**];

(d) verifying the authentication of said first identity device *[[chip card]]* relative to said privacy reference point from said first identity device *[[chip card]]* **[Herz: Col. 30, line 39-43; Col. 37, lines 48-53; "The proxy server may verify those credentials and make appropriate modifications to the user's profile as required by these credentials such as recording the user's new demographic status as an adult. It may also store those credentials, so that it can present them to service providers on the user's behalf"**]; and

(e) establishing a second communication path from a first communication device associated with a first entity to said privacy reference point through said data communication network **[Herz: Col. 31, line 57 to Col. 32, line 2; "service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore, must provide the service provider with proof of funds (a credential) from the bank, while *still not disclosing the user's true identity* to the service provider"; *a first communication device is equivalent to a service provider*].**

(f) wherein at least one of the steps of verifying the authentication and establishing a second communication is performed **[Herz: Col. 30, line 39-43; Col. 37, lines 48-53; "The proxy server may verify those credentials and make appropriate modifications to the user's profile as required by these credentials such as recording the user's new demographic status as an adult. It may also store those credentials, so that it can present them to service providers on the user's behalf"]** *[[without disclosing the identity of said chip card]].*

Herz discloses the privacy reference point and the steps of verifying the authentication and establishing a second communication is performed but does not explicitly disclose the privacy reference point is configured for use in one transaction and without disclosing the identity of said first identity device.

However, Pfitzmann teaches Anonymity, Unobservability, and Pseudonymity wherein one-time-use pseudonym is used in one transaction pseudonym without disclosing the identity of said first identity device **[Pfitzmann: pg. 6-7; Different pseudonym is used for each transaction, there is no possibility to link different transactions by equality of the pseudonyms].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Herz by including the teaching of Pfitzmann because it would provide a different transaction pseudonym is used, e.g. randomly generated transaction numbers for online-banking. Thus, there is at least no possibility to link different transactions by equality of pseudonyms. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible **[Pfitzmann, pg. 6, transaction pseudonym section].**

Pfitzmann does not explicitly disclose a first identity device which is a chip card.

However, Engberg teaches Privacy Authentication – persistent non-identification in Ubiquitous environments wherein first identity device is a chip card **[Engberg: pg. 4; "These operation should be controlled o a tamper-resistant environment such as *smart-card (i.e. chip card)* together with additional protection."].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Herz and Pfitzmann by including the teaching of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

As per claim 21:

The combination of Herz, Pfitzmann, and Engberg teach the subject as described above.

Herz further teaches the method according to claim 20, wherein the step of providing an authentication comprises the steps of:

registering data selected from the group consisting of biometrics, a signature, a code, and any combinations thereof and comparing the registered data with corresponding stored data **[Herz: Col. 31, lines 53-63; "A second and equally important requirement of a pseudonym system is that it provide for digital credentials, which are used to guarantee that the user represented by a particular pseudonym has certain properties. These credentials may be granted on the basis of result of activities and transactions conducted by means of the system for customized electronic identification of desirable objects, or on the basis of other activities and transactions conducted on the network N of the present system, on the basis**

of users' activities outside of network N"].

As per claim 22:

The combination of Herz, Pfitzmann, and Engberg teach the subject as described above.

The combination of Herz and Engberg further teach the method of claim 20, wherein the step of verifying the authentication is performed without disclosing the identity of said chip card **[Herz: Col. 31, line 57 to Col. 32, line 2; "service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore, must provide the service provider with proof of funds (a credential) from the bank, while still not disclosing the user's true identity to the service provider"; a second identity device is equivalent to a service provider; Engberg: pg. 4; "These operation should be controlled o a tamper-resistant environment such as *smart-card (i.e. chip card)* together with additional protection."].**

As per claim 23:

The combination of Herz, Pfitzmann, and Engberg teach the subject as described above.

The combination of Herz and Engberg further teach the method of claim 20, wherein the step of establishing a second communication path is performed without disclosing the identity of said chip card **[Herz: Col. 31, line 57 to Col. 32, line 2; "service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore,**

must provide the service provider with proof of funds (a credential) from the bank, while still not disclosing the user's true identity to the service provider"; a second identity device is equivalent to a service provider; Engberg: pg. 4; "These operation should be controlled o a tamper-resistant environment such as *smart-card (i.e. chip card)* together with additional protection."].

As per claim 24:

The combination of Herz, Pfitzmann, and Engberg teach the subject as described above. Enberg further teach the method according to claim 20, wherein said chip card includes encrypted data, said method further comprising:

(a) said chip card receiving an encrypted key from said privacy reference point **[Engberg: pg. 1 ; abstract, user identifiers; pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc"; pg. 4; "These operation should be controlled o a tamper-resistant environment such as *smart-card (i.e. chip card)* together with additional protection."]**;

(b) decrypting said encrypted key using a second stored key to create a decrypted version of the encrypted key **[Engberg: pg. 1 ; abstract, user identifiers; pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc"]**; and

(c) decrypting said encrypted data using the decrypted version of said encrypted key

[Engberg: pg. 1 ; abstract, user identifiers; pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc"].

As per claim 25:

The combination of Herz, Pfitzmann, and Engberg teach the subject as described above.

Enberg the method according to claim 20, the communication network being selected from a group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof **[Engberg: pg. 1; "In ubiquitous computing macro (long-distance GSM, UMTS etc.) wireless communication is integrating with micro (local Bluetooth, infrared etc.) wireless communication as part of users general identity end environment management"].**

As per claim 26:

The combination of Herz, Pfitzmann, and Engberg teach the subject as described above.

The combination of Herz, Pfitzmann, and Engberg further teach the method according to claim 20, said chip card having an authenticated holder, and said privacy reference point being addressable by the authenticated holder from a computer communicating with said data

communication network [**Herz: fig. 2; Col. 30, lines 39-47; a smart cards (i.e. authenticated holder); Col. 32, lines 3-65; "our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the implementation of a set of one or more proxy servers distributed throughout the network N. …. Proxy servers may be the same or different"; Pfitzmann: pg. 6-7; Different pseudonym is used for each transaction, there is no possibility to link different transactions by equality of the pseudonyms; Engberg: pg. 4; "These operation should be controlled o a tamper-resistant environment such as *smart-card (i.e. chip card)* together with additional protection."**].

As per claim 27:

The combination of Herz, Pfitzmann, and Engberg further teach the subject as described above.

Enberg further teaches the method according to 20, further comprising said chip card allowing or blocking access to said privacy reference point by second communication device **[Engberg: pg. 2, "The outcome is a setup in which a PAD device can establish an authenticated wireless IP-session with the normal subscription telecom provider (STP) without the STP having any persistent device or user identifier to link one session with a PAD-device to the next and still have traceability in case the PAD-device user is involved in any criminal activity"].**

As per claim 29:

The combination of Herz, Pfitzmann, and Engberg further teach the subject as described above.

Engberg further teaches the method according to claim 20, wherein at least one of said steps of establishing a first communication path and establishing a second communication path involves creating and negotiating an accountability path adapted to a context risk profile **[Engberg: pg. 3, "Key to Privacy Authentication is the existence of Privacy Accountability. The various properties of Privacy Accountability including how it could be established are not discussed in this paper even though it is highly relevant. We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym. The data component is encrypted using multiple layers in such a way that it is not providing linkability by its existence and only through a series of steps including multiple trusted parts lead to disclosure of identity or other linking information ... Relevant for this paper is the consideration that possession of a data component providing such properties is not in itself identifying as identity is not readily accessible nor is it clearly anonymous as linkability exists. Privacy Accountability is structurally different from an Identity Escrow setup as in a PKI Certificate Authority as the unit in possession of the data component are only trusted to keep the data component in hiding until the disclosure process - for any reason – is required to initiate"]**.

<u>As per claim 30:</u>

The combination of Herz, Pfitzmann, and Engberg further teach the subject as described above.

Enberg further teaches the method according to claim 29, wherein said chip card has an authenticated holder, and said first communication device establishes a procedure to identify a party selected from a group consisting of said chip card and the authenticated holder of said chip card **[Engberg: pg. 3-4; "Key to Privacy Authentication is the existence of Privacy Accountability. The various properties of Privacy Accountability including how it could be…These operations should be controlled in a tamper-resistant environment such as a smart-card (i.e. authenticated holder) together with additional protection; pg. 4; "These operation should be controlled o a tamper-resistant environment such as *smart-card (i.e. chip card)* together with additional protection."]**.

As per claim 31:

The combination of Herz, Pfitzmann, and Engberg further teach the subject as described above. Enberg further teaches the method according to claim 30, wherein said procedure to identify a party employs identification information selected from a group consisting of at least one of biometrics, name, digital signature, and a code **[Engberg: pg. 3, "We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym"]**.

As per claim 33:

Claim 33 is essentially the same as claim 20 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 34:

Claim 34 is essentially the same as claim 21 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 38:

Claim 38 is essentially the same as claim 22 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 39:

Claim 39 is essentially the same as claim 23 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over by **Herz** et al. (5,754,938) in view of **Andreas Pfitzmann** et al, Anonymity, *Unobservability, and Pseudonymity - A Proposal for Terminology, LNCS 2009, pages 1-9, 2001,* further in view of **Engberg** et al. ("Privacy Authentication – persistent non-identification in Ubiquitous environments", August 18, 2002, pages 1-6), and further in view of **Busboon** (US 2006/0155993 A1).

As per claim 32:

The combination of Herz, Pfitzmann, and Engberg further teach the subject as described above.

Enberg further teaches,

(f) transmitting information from said first communication device to said service provider **[Engberg: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**;

(g) transmitting said information from said service provider to said identity provider **[Engberg: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**;

(h) transmitting said information from said identity provider to said further communication device **[Engberg: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**;

(l) said further communication device responding to said information by transmitting a payment acceptance to said identity provider **[Engberg: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**;

(m) said identity provider transmitting said payment acceptance to said service provider **[Engberg: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the**

Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]; and

(n) said service provider transmitting said payment acceptance to said first communication device **[Engberg: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**.

Herz and Pfitzmann do not explicitly disclose,

(a) providing an identity provider and a service provider;

(b) establishing communication from said first communication device to said service provider;

(c) establishing communication from said service provider to said identity provider;

(d) providing a further communication device associated with a financial institution;

(e) establishing communication from said service provider to said further communication device.

However, Busboon teaches service provider anonymous in a single sign-on system wherein

(a) providing an identity provider and a service provider **[Busboon: par. [0024]; a communication between service provider and identity provide]**;

(b) establishing communication from said first communication device to said service provider **[Busboon: par. [0024]; a communication between service provider and identity provide]**;

(c) establishing communication from said service provider to said identity provider **[Busboon: par. [0024]; a communication between service provider and identity provide]**;

(d) providing a further communication device associated with a financial institution **[Busboon: par. [0094]; service provider can further retrieve specific profile information for the client currently requesting a service, for example, a customized portal, access to bank account and the like]**;

(e) establishing communication from said service provider to said further communication device **[Busboon: par. [0094]; service provider can further retrieve specific profile information for the client currently requesting a service, for example, a customized portal, access to bank account and the like]**.

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Herz, Pfitzmann, and Engberg by including the teaching of Busboon because it would provide solutions for privacy and data protection problems **[par. [0023], Busboon].**

(B) Second ground rejection:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 20-27, 29-31, and 33-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stephan J. Engberg (WO 01/90968 A1, November 2001), hereinafter as **Engberg-1** in view of Andreas **Pfitzmann** et al, Anonymity, *Unobservability, and Pseudonymity - A Proposal for Terminology, LNCS 2009, pages 1-9, 2001*

As per claim 20:

Engberg-1 teaches a method of establishing a communication path in a data communication network from a chip card associated with a client, comprising the steps of:

(a) providing a privacy reference point in said data communication network, said privacy reference point configured for use in one transaction **[Engberg-1: abstract: Privacy is established using a principle of multiple *non-linkable pseudonyms* or *Virtual Identities (VID)*; See also pg. 35 , lines 10-23; Virtual Identity; pg. 33, Zero-knowledge generation of *on-time-only keys*; See also pg. 106, lines 25 to pg. 107, lines 32; *one-time-only VID*; pg. 131, lines 15-20; pg. 38]**;

(b) establishing a first communication path from said chip card to said privacy reference point [**Engberg-1: abstract: pg. 6, lines 3-12; providing a first virtual identifier of *the first legal entity* to the second legal entity, and establishing *a communication path* in according with a set of communication Rules specified by *the first legal entity*; See also; pg. 17; "The mobile processing and memory unit according to the fourth aspect of the invention may comprises *SmartCard* enabling Zero-knowledge authentication; pgs. 33, 56, 58, 76; Smartcard (i.e. chip card)]**.

(c) providing an authentication of the said chip card relative to the privacy reference point **[Engberg-1: abstract; pg. 6 line 21 to pg. 7, line 11; providing second legal entity with *authentication or profile information* related to said communication path and/or first legal entity; A preferred embodiment involves providing a Virtual Identifier equaling *establishing an authenticated yet anonymous* session in any kind of communication path; See also pg. 16, line 5 to pg. 17, line 8; *authentication unit* enabling the first client establishing *a first virtual identity* having a first virtual communication channel and establishing a rule based communication routing scheme for the privacy communication channel; pg. 56; tamper-safe *SmartCards* with a encryption authentication mechanism that can be either standard signature or a more complex zero-knowledge authentication procedure. See for instance [S.A. Brands 1999 PHD thesis later published as "Re-thinking Public and Digital Certificate", MIT Press, 2000, ISBN 0-262-02491-8"]**;

(d) verifying the authentication of said chip card relative to said privacy reference point from said chip card **[Engberg-1: abstract; pg. 6 line 21 to pg. 7, line 11; providing second legal entity with *authentication or profile information* related to said communication path and/or first legal entity; A preferred embodiment involves providing a Virtual Identifier equaling *establishing an authenticated yet anonymous* session in any kind of communication path; See also pg. 16, line 5 to pg. 17, line 8; *authentication unit* enabling the first client establishing *a first virtual identity* having a first virtual communication channel and establishing a rule based communication routing scheme for the privacy communication channel; pg. 56; tamper-safe *SmartCards* with a encryption authentication mechanism that can be either standard signature or a more complex zero-knowledge authentication**

procedure. See for instance [S.A. Brands 1999 PHD thesis later published as "Re-thinking Public and Digital Certificate", MIT Press, 2000, ISBN 0-262-02491-8"]; and

(e) establishing a second communication path from a first communication device associated with a first entity to said privacy reference point through said data communication network **[Engberg-1: abstract: pg. 6, lines 3-12; providing a first virtual identifier of *the first legal entity* to the second legal entity, and establishing *a communication path* in according with a set of communication Rules specified by *the first legal entity* between *the first and the second legal entity*]**;

(f) wherein at least one of the steps of verifying the authentication and establishing a second communication is performed without disclosing the identity of said chip card **[Engberg-1: abstract: pg. 6, lines 3-12; the first legal entity *is remaining anonymous*** (i.e. without disclosing the identity) **to the second entity; See also pg. 7, lines 18-21]**.

Engberg-1 discloses a privacy which is established using a principle of multiple non-linkable pseudonym or Virtual Identifies (VID) **[Engberg-1; pg. 5, lines 5-13]** but not in details one-time-use pseudonym (i.e. one-time-use reference ("privacy reference point")).

However, Pfitzmann teaches Anonymity, Unobservability, and Pseudonymity wherein one-time-use pseudonym is used in one transaction pseudonym disclosing the identity of said a first identity device **[Pfitzmann: pg. 6-7; transaction pseudonym: Different pseudonym is used for each transaction, there is no possibility to link different transactions by equality of the pseudonyms. Transaction pseudonyms can be used to realize as strong *anonymous* as possible].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Engberg-1 by including the teaching of Pfitzmann because it would provide a different transaction pseudonym is used, e.g. randomly generated transaction numbers for online-banking. Thus, there is at least no possibility to link different transactions by equality of pseudonyms. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible **[Pfitzmann, pg. 6, transaction pseudonym section].**

As per claim 21:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to claim 20, wherein the step of providing an authentication comprises the steps of:

(a) registering data selected from the group consisting of biometrics, a signature, a code, and any combinations thereof **[Engberg-1: pg. 43, lines 7-23; *Biometrics*; pg. 31, line 15 to pg. 32 line 16; *verifying a signature* made by the private key without knowing the private key; pg. 57, lines 112; *Biometrics* like a *fingerprint reader*; See also, g. 127, lines 26-30]**; and

(b) comparing the registered data with corresponding stored data **[Engberg-1: pg. 31, line 15 to pg. 32 line 16; *verifying a signature* made by the private key without knowing the private key]**.

As per claim 22:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above.

Engberg-1 further teaches the method of claim 20, wherein the step of verifying the authentication is performed without disclosing the identity of said chip card [**Engberg-1: abstract: pg. 6, lines 3-12; the first legal entity *is remaining anonymous*** (i.e. without disclosing the identity) **to the second entity; See also pg. 7, lines 18-21; pg. 6 line 21 to pg. 7, line 11; providing second legal entity with *authentication or profile information* related to said communication path and/or first legal entity; A preferred embodiment involves providing a Virtual Identifier equaling *establishing an authenticated yet anonymous* session in any kind of communication path; pg. 56; tamper-safe *SmartCards* with a encryption authentication mechanism that can be either standard signature or a more complex zero-knowledge authentication procedure. See for instance [S.A. Brands 1999 PHD thesis later published as "Re-thinking Public and Digital Certificate", MIT Press, 2000, ISBN 0-262-02491-8"**].

<u>As per claim 23:</u>

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method of claim 20, wherein the step of establishing a second communication path is performed without disclosing the identity of said chip card [**Engberg-1: abstract: pg. 6, lines 3-12; the first legal entity *is remaining anonymous*** (i.e. without disclosing the identity) **to the second entity; See also pg. 7, lines 18-21; pg. 6 line 21 to pg. 7, line 11; providing second legal entity with *authentication or profile information* related to said communication path and/or first legal entity; A preferred embodiment involves providing a Virtual Identifier equaling *establishing an authenticated yet anonymous* session**

in any kind of communication path; pg. 56; tamper-safe *SmartCards* with a encryption authentication mechanism that can be either standard signature or a more complex zero-knowledge authentication procedure. See for instance [S.A. Brands 1999 PHD thesis later published as "Re-thinking Public and Digital Certificate", MIT Press, 2000, ISBN 0-262-02491-8"].

As per claim 24:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to claim 20, wherein said chip card includes encrypted data, said method further comprising:

(a) said chip card receiving an encrypted key from said privacy reference point **[Engberg-1: pg. 39, line 15-21; CLIENT can attach multiple symmetric encryption keys to a RELATION for communication encryption. *Keys are encrypted using encryption keys* not known by TP]**;

(b) decrypting said encrypted key using a second stored key to create a decrypted version of the encrypted key **[Engberg-1: pg. 53; liens 20-26; Decryption keys are stored either CLIENT side or together with the data in encrypted form using the Public part of the CLIENT Digital Signature]**; and

(c) decrypting said encrypted data using the decrypted version of said encrypted key **[Engberg-1: pg. 136; lines 3-31; CLIENT can verify that Credentials is anonymous and correct by decrypting the Credential using the public key of third-party]**.

As per claim 25:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to claim 20, the communication network being selected from a group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network **[Engberg-1: pg. 126, lines 14-17; "The communication oath can be based on a large variety of network protocols such as *wireless* in the form of Bluetooth, Infrared, GSM, WAP, GPRS, Wireless IP]**, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof.

As per claim 26:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to 20, said chip card having an authenticated holder, and said privacy reference point being addressable by the authenticated holder from a computer communicating with said data communication network **[Engberg-1: pg. 34, lines 15-18; Attribute Certificate are a special type of anonymous certificates where *the holder* is able to demonstrate to *third-party* with zero-knowledge communication that he hold or does not hold a certain credential]**.

As per claim 27:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above.

Engberg-1 further teaches the method according to claim 20, further comprising said chip card allowing or blocking access to said privacy reference point by second communication device **[Engberg-1: pg. 34, lines 15-18; Attribute Certificate are a special type of anonymous certificates where *the holder* is able to demonstrate to *third-party* with zero-knowledge communication that he hold or does not hold a certain credential]**.

As per claim 29:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to claim 20, wherein at least one of said steps of establishing a first communication path and establishing a second communication path involves creating and negotiating an accountability path adapted to a context risk profile **[Engberg-1: pg. 4, lines 18-21; accountability in case of fraud as defined by law; pg. 17, line 7 to pg. 18, line 2; The system may provide the client with full privacy control of the first client identity and information related to the first client, however, the information is subject to *basic accountability principles;* See also pg. 19, lines 27-31; pg. 122, line 24 to pg. 123, line 20]**.

As per claim 30:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to claim 29, wherein said chip card has an authenticated holder, and said first communication device establishes a procedure to identify a party selected from a group consisting of said chip card and the authenticated holder of said chip card **[Engberg-1: pg. 17, line 10-12; Smartcard (i.e. authentication holder) enabling Zero-**

knowledge authentication; pg. 123, line 31 to pg. 124, line 2]..

As per claim 31:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further teaches the method according to claim 30, wherein said procedure to identify a party employs identification information selected from a group consisting of at least one of biometrics, name, digital signature, and a code **[Engberg-1: pg. 43, lines 7-23; *Biometrics*; pg. 31, line 15 to pg. 32 line 16; *verifying a signature* made by the private key without knowing the private key; pg. 57, lines 112; *Biometrics* like a *fingerprint reader*; See also, g. 127, lines 26-30]**.

As per claim 33:

Claim 33 is essentially the same as claim 20 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 34:

Claim 34 is essentially the same as claim 21 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 38:

Claim 38 is essentially the same as claim 22 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 39:

Claim 39 is essentially the same as claim 23 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 35:

Claim 35 is essentially the same as claim 25 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 36:

Claim 36 is essentially the same as claim 24 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

As per claim 37:

Claim 37 is essentially the same as claim 31 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stephan J. Engberg (WO 01/90968 A1, November 2001), hereinafter as **Engberg-1** in view of Andreas **Pfitzmann** et al, *"Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology"*, LNCS 2009, pages 1-9, 2001, further in view of **Busboon** (US 2006/0155993 A1), and further in view

of Engberg et al. *("Privacy Authentication – persistent non-identification in Ubiquitous environments", August 18, 2002, pages 1-6)* hereinafter as **Engberg-2**,

As per claim 32:

The combination of Engberg-1 and Pfitzmann teach the subject matter as described above. Engberg-1 further discloses transferring a financial instrument to the second legal entity, requesting confirmation of payment from the third legal entity **[Engberg-1: fig. 32; pg. 12, lines 1-13]**.

Engberg-1 does not explicit disclose in details,

(a) providing an identity provider and a service provider;

(b) establishing communication from said first communication device to said service provider;

(c) establishing communication from said service provider to said identity provider;

(d) providing a further communication device associated with a financial institution;

(e) establishing communication from said service provider to said further communication device;

(f) transmitting information from said first communication device to said service provider;

(g) transmitting said information from said service provider to said identity provider;

(h) transmitting said information from said identity provider to said further communication device;

(l) said further communication device responding to said information by transmitting a payment acceptance to said identity provider;

(m) said identity provider transmitting said payment acceptance to said service provider; and

(n) said service provider transmitting said payment acceptance to said first communication device.

However, Busboon teaches service provider anonymous in a single sign-on system wherein,

(a) providing an identity provider and a service provider **[Busboon: par. [0024]; a communication between service provider and identity provide]**;

(b) establishing communication from said second identity device to said service provider **[Busboon: fig. 1; par. [0024]; a communication between service provider and identity provide]**;

(c) establishing communication from said service provider to said identity provider **[Busboon: fig. 1; par. [0024]; a communication between service provider and identity provide]**;

(d) providing a further identity device corresponding to a financial institution **[Busboon: par. [0094]; service provider can further retrieve specific profile information for the client currently requesting a service, for example, a customized portal, access to bank account and the like]**;

However, Busboon teaches service provider anonymous in a single sign-on system wherein,

(a) providing an identity provider and a service provider **[Busboon: par. [0024]; a communication between service provider and identity provide]**;

(b) establishing communication from said first communication device to said service provider **[Busboon: fig. 1; par. [0024]; a communication between service provider and identity provide]**;

(c) establishing communication from said service provider to said identity provider **[Busboon: fig. 1; par. [0024]; a communication between service provider and identity provide]**;

(d) providing a further communication device associated with a financial institution **[Busboon: par. [0094]; service provider can further retrieve specific profile information for the client currently requesting a service, for example, a customized portal, access to bank account and the like]**;

(e) establishing communication from said service provider to said further communication device **[Busboon: par. [0094]; service provider can further retrieve specific profile information for the client currently requesting a service, for example, a customized portal, access to bank account and the like]**;

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Engberg-2 by including the teaching of Busboon because it would provide solutions for privacy and data protection problems **[par. [0023], Busboon].**

Engberg-1 and Busboon do not explicitly disclose in details,

(f) transmitting information from said first communication device to said service provider;

(g) transmitting said information from said service provider to said identity provider;

(h) transmitting said information from said identity provider to said further communication device;

(l) said further communication device responding to said information by transmitting a payment acceptance to said identity provider;

(m) said identity provider transmitting said payment acceptance to said service provider; and

(n) said service provider transmitting said payment acceptance to said first communication device.

However, Engberg-2 teaches Privacy authentication – persistent non-identification in Ubiquitous environments, wherein

(f) transmitting information from said first communication device to said service provider **[Engberg-2: pg. 5; "The Subscription Telecom receive a request for establishing a session together with a reference to the Privacy Authenticating Unit (PAU) able to authenticate the user. The Subscription Telecom establish an IP-session through the Subscription Telecom to the Privacy Authentication Unit limited to the authentication process only"]**;

(g) transmitting said information from said service provider to said identity provider **[Engberg-2: pg. 5; "The Subscription Telecom receive a request for establishing a session together with a reference to the Privacy Authenticating Unit (PAU) able to authenticate the**

user. The Subscription Telecom establish an IP-session through the Subscription Telecom to the Privacy Authentication Unit limited to the authentication process only"];

(h) transmitting said information from said identity provider to said further communication device **[Engberg-2: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**;

(l) said further communication device responding to said information by transmitting a payment acceptance to said identity provider **[Engberg-2: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**;

(m) said identity provider transmitting said payment acceptance to said service provider **[Engberg-2: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**; and

(n) said service provider transmitting said payment acceptance to said first communication device **[Engberg-2: pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Engberg-1 and Busboon by including the teaching of Engberg-2 because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg-2].**

Conclusion

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

April 7, 2010

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439